IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

MATTHEW TURTURRO, on behalf of himself and all others similarly situated, Plaintiff, v. NATIONSTAR MORTGAGE, LLC d/b/a MR. COOPER and MR. COOPER GROUP, INC., Defendants.	**Case No. _____** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Matthew Turturro ("Plaintiff") brings this Class Action Complaint on behalf of himself, and all others similarly situated, against Defendants Nationstar Mortgage, LLC, d/b/a Mr. Cooper ("Nationstar") and Mr. Cooper Group, Inc. (collectively, "Defendants" or "Mr. Cooper"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge:

NATURE OF THE CASE

1. Mr. Cooper is the third-largest mortgage servicer in the United States with more than 4.3 million customers nationwide.

2. During the course of its operations, Mr. Cooper acquired, collected, stored, utilized, and derived a benefit from Plaintiff's and Class Members' first and last names, addresses, states of residence, phone numbers, dates of birth, bank account, and other financial information, and Social Security numbers (collectively, the "Personally Identifiable Information" or "PII").

3. Mr. Cooper, therefore, owed and otherwise assumed non-delegable statutory, regulatory, and common law duties and obligations, including to keep Plaintiff's and Class Members' PII confidential, safe, secure, and protected from the type of unauthorized access, disclosure, and theft that occurred in this matter.

4. This duty arises based upon the parties' relationship and because it is foreseeable that the exposure of PII to unauthorized persons—and especially cybercriminals with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private matters.

5. This harm manifests in several ways, as the exposure of a person's PII through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives.

6. On October 31, 2023, Mr. Cooper suffered a data breach in which an unauthorized third party gained access to certain of Mr. Cooper's technology systems (the "Data Breach"). Following detection, Mr. Cooper shut down certain of its systems.

7. Plaintiff brings this class action on behalf of customers of Mr. Cooper whose PII was accessed and exposed to unauthorized third parties during the Data Breach of Mr. Cooper's systems and servers.

8. Plaintiff, on behalf of himself and the Class as defined herein, bring claims for negligence, negligence *per se*, violation of the consumer protection laws of New York, and declaratory and injunctive relief, seeking actual, compensatory, punitive, and nominal damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and relief.

9. As a direct and proximate result of Mr. Cooper's inadequate data security, its breach of its duty to handle PII with reasonable care, and its failure to maintain the confidentiality of customers' information, Plaintiff's and Class Members' PII has been accessed by hackers and exposed to an untold number of unauthorized individuals.

10. Plaintiff and Class Members are now at a significantly increased risk of fraud, identity theft, intrusion of their privacy, and similar forms of criminal mischief, which risk may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy protecting themselves, to the extent possible, from these crimes.

11. To recover from Defendants for these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, along with injunctive relief requiring Defendants to, at minimum: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) disclose, expeditiously, the full nature of the Data Breach and the types of PII accessed, obtained, or exposed by the hackers; and (iv) provide lifetime monitoring and identity theft insurance to all Class Members.

PARTIES

A. Plaintiff

12. Plaintiff Matthew Turturro is an adult individual who is a citizen of New York and currently resides in Richmond County, New York. Plaintiff's PII was maintained within Defendants' networks and servers, as Plaintiff is a customer of Mr. Cooper.

13. Plaintiff's relationship with Mr. Cooper began in approximately June 2023, when his mortgage was involuntarily transferred from Wells Fargo to Mr. Cooper to be Plaintiff's new mortgage servicer.

14. On or around November 2, 2023, Plaintiff received a notice email from Mr. Cooper, informing him of the Data Breach and that Mr. Cooper had "locked down" its systems. Since Plaintiff manually pays his mortgage each month Plaintiff is uncertain if Mr. Cooper will timely receive and process Plaintiff's upcoming November payment given their system outages.

15. In response and as a result of the Data Breach, Plaintiff and Class Members have spent significant time and effort researching the Data Breach and reviewing and monitoring their accounts for fraudulent activity.

16. Plaintiff and Class Members suffered actual damages as a result of the failures of Defendants to adequately protect the sensitive information entrusted to it, including, without limitation, experiencing fraud or attempted fraud, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identity theft.

17. As a result of the Data Breach, Plaintiff and Class Members have been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending and is not speculative given the highly sensitive nature of the PII compromised by the Data Breach.

B. Defendants

18. Defendant Nationstar Mortgage, LLC d/b/a Mr. Cooper ("Nationstar") is a Delaware limited liability company with its principal place of business in Coppell, Dallas County, Texas. Nationstar is the operating subsidiary of parent Defendant Mr. Cooper Group, Inc. Nationstar is registered to do business with the Texas Secretary of State.

19. Defendant Mr. Cooper Group, Inc. is incorporated in Delaware with its principal place of business in Coppell, Dallas County, Texas. Mr. Cooper Group, Inc. is the operating parent of subsidiary Nationstar. Mr. Cooper Group, Inc. is registered to do business with the Texas Secretary of State.

JURISDICTION AND VENUE

20. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000, exclusive of interest and costs, there are more than 100 putative Members of the Class defined below, and a significant portion of putative Class Members are citizens of a different state than Defendants.

21. This Court has personal jurisdiction over Defendants because Defendant Nationstar and Defendant Mr. Cooper Group, Inc. are each registered to do business with the Texas Secretary of State, are headquartered and have their principal place of business of and/or routinely conduct business in the Dallas Division of the Northern District of Texas, have sufficient minimum contacts in Texas, have intentionally availed themselves of this jurisdiction by marketing and/or selling products and/or services and/or by accepting and processing payments for those products and/or services within Texas. Furthermore, Texas's long-arm statute provides for jurisdiction to the fullest extent allowed under the Constitution of the United States based on the most minimum contact with Texas as torts were committed in whole or in part in Texas. *See* Tex. Civ. Prac. & Rem. Code Ann. § 17.042.

22. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL BACKGROUND

A. The Mr. Cooper Data Breach

23. On November 2, 2023, Mr. Cooper announced via an 8-K securities filing with the SEC that on October 31, 2023, Mr. Cooper experienced a "cybersecurity incident" in which "an unauthorized third party gained access to certain technology systems."

24. Mr. Cooper began notifying its customers of the Data Breach, including Plaintiff, by email on or around November 2, 2023.

25. According to its 8-K, following detection of the incident, Mr. Cooper "initiated response protocols," including "containment measures" and "shutting down" certain of its systems.

26. Since shutting down their systems, mortgage customers attempting to log in to Mr. Cooper's website to pay their mortgages or loans were greeted with a message stating that the company was suffering a technical outage and could not make payments via the website.

27. Mr. Cooper's systems were not accessible from November 1 through 4, 2023, and many customers were unable to make payments or access their accounts.

28. On November 9, 2023, Mr. Cooper confirmed via an 8-K securities filing with the SEC that Mr. Cooper's "preliminary analysis found that certain customer data was exposed," in the Data Breach.

29. The Data Breach occurred as a direct result of Defendants' failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect its customers' PII.

30. Like Plaintiff, the Class Members received similar notices informing them that their PII was exposed in the Data Breach.

B. Defendants Knew the Risks of Storing Valuable PII and the Foreseeable Harm to Victims

31. At all relevant times, Defendants knew it was storing and permitting its internal networks and servers to transmit valuable, sensitive PII and that, as a result, Defendants' systems would be attractive targets for cybercriminals.

32. Defendants also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, as well as intrusion into their highly private financial information.

33. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, and many others.

34. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[1]

35. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the United States.

36. According to the Identity Theft Resource Center, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.[2]

[1] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.
[2] *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, *available at* https://notified.idtheftcenter.org/s/resource#annualReportSection.

37. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[3]

38. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[4]

39. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

40. Plaintiff was and is very careful about sharing his PII. Plaintiff took reasonable steps to maintain the confidentiality of his PII and relied on Defendants to keep his PII confidential

[3] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1).
[4] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf.

and securely maintained, to use this information for related business purposes only, and to make only authorized disclosures of this information.

41. Plaintiff and Class Members provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

C. Defendants Failed to Comply with the FTC Act

42. Defendants are prohibited by the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45 (Section 5 of the FTC Act), from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

43. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice that violates the FTC Act.

44. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

45. In 2007, the FTC published guidelines establishing reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose

a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

46. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

47. Defendants are aware of and failed to follow the FTC guidelines and failed to adequately secure PII.

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

49. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII, or to prevent the disclosure of such information to unauthorized individuals constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

50. Defendants were at all times fully aware of their obligations to protect the PII of consumers because of its business of obtaining, collecting, and storing PII. Defendants were also aware of the significant repercussions that would result from their failure to do so.

D. Plaintiff and Class Members Suffered Damages

51. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways.

Plaintiff and Class Members must immediately devote time, energy, and money to: 1) closely monitor their account statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

52. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendants' conduct. Further, the value of Plaintiff's and Class Members' PII has been diminished by its exposure in the Data Breach.

53. As a result of Defendants' failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII.

54. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[5]

55. Plaintiff and the Class members have also been injured by Defendants' unauthorized disclosure of their confidential and private financial records and PII.

56. Plaintiff and Class Members are also at a continued risk because their information remains in Defendants' systems, which have already been shown to be susceptible to compromise

[5] *See* https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.

and attack and are subject to further attack so long as Defendants fail to undertake the necessary and appropriate security and training measures to protect its customers' PII.

CLASS ACTION ALLEGATIONS

57. Plaintiff brings this action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and (b)(3), individually and on behalf of the following Nationwide Class:

> All persons whose PII was compromised in Defendants' Data Breach that was announced on or about November 2, 2023 (the "Nationwide Class").

58. Plaintiff brings this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and (b)(3) on behalf of the following New York Subclass:

> All persons in New York whose PII was compromised in Defendants' Data Breach that was announced on or about November 2, 2023 (the "New York Subclass").

59. Excluded from the Class are Defendants, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

60. **Numerosity**. All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The class described above is so numerous that joinder of all individual members in one action would be impracticable. While Plaintiff is informed and believes that there are likely hundreds of thousands of members of the Class, the precise number of Class members is unknown to Plaintiff. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendants' records, including but not limited to, the files implicated in the Data Breach.

61. **Commonality and Predominance**. All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves questions of law and fact that are common to the Class Members. Such common questions predominate over any issues affecting only individual Class Members and include, but are not limited to:

a. Whether Defendants had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendants had a duty to maintain the confidentiality of Plaintiff's and Class Members' PII;

c. Whether Defendants breached their obligation to maintain Plaintiff's and the Class Members' PII in confidence;

d. Whether Defendants were negligent in collecting and storing Plaintiff's and Class Members' PII, and breached its duties thereby;

e. Whether Defendants failed to properly give notice pursuant to state and/or federal law;

f. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conduct; and

g. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

62. **Typicality**. All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of the Class Members. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendants to safeguard PII. Plaintiff and Class Members were all customers of Defendant, each having their PII obtained by an unauthorized third party.

63. **Adequacy of Representation**. All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members that Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation, including data breach litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

64. **Predominance and Superiority.** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiff's case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Members of the Class to individually seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

65. **Cohesiveness**. All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendants have acted, or refused to act, on grounds generally applicable to the Nationwide Class and Subclass such that final declaratory or injunctive relief is appropriate.

66. Plaintiff reserves the right to modify, amend, or revise the foregoing class allegations and definitions prior to moving for class certification based on newly learned facts or legal developments that arise following additional investigation, discovery, or otherwise.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(By Plaintiff on behalf of the Nationwide Class, or, alternatively, the New York Subclass)

67. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

68. Defendants owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

69. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

70. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendants. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

71. Defendants' duty also arose from Defendants' position as a provider of mortgage servicing. Defendants hold themselves out as a trusted provider of servicing customers' mortgages, and they thereby assumed a duty to reasonably protect their customers' information.

72. Indeed, Defendants, as a direct mortgage servicer, were in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

73. Defendants were subject to an "independent duty" between Plaintiff and Class Members and Defendants.

74. Defendants violated their own policies by actively disclosing Plaintiff's and the Class Members' PII; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII; failing to maintain the confidentiality of Plaintiff's and the Class Members' records; and by failing to provide timely notice of the breach of PII to Plaintiff and the Class.

75. Defendants breached the duties owed to Plaintiff and Class Members and thus were negligent. Defendants breached these duties by, among other things:

a. mismanaging their system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII;

b. mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein; and

f. failing to detect the breach at the time it began or within a reasonable time thereafter.

76. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, their PII would not have been compromised.

77. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i. Loss of their privacy and confidentiality in their PII;

j. The erosion of the essential and confidential relationship between Defendants – as a mortgage servicer – and Plaintiff and Class members as customers; and

k. Loss of personal time spent carefully reviewing financial statements to check for charges for services not received.

78. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including actual, compensatory, punitive, and nominal damages, in an amount to be proven at trial.

79. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) disclose, expeditiously, the

full nature of the Data Breach and the types of PII accessed, obtained, or exposed by the hackers; and (iv) provide lifetime monitoring and identity theft insurance to all Class Members.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(By Plaintiff on behalf of the Nationwide Class, or, alternatively, the New York Subclass)

Negligence *Per Se* Under the FTC Act

80. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

81. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendants or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

82. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach involving PII of its customers.

83. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

84. The harm that has occurred as a result of Defendants' conduct is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

85. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including actual, compensatory, punitive, and nominal damages, in an amount to be proven at trial.

86. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

87. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) disclose, expeditiously, the full nature of the Data Breach and the types of PII accessed, obtained, or exposed by the hackers; and (iv) provide lifetime monitoring and identity theft insurance to all Class Members.

THIRD CAUSE OF ACTION
NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. Law §§ 349, *et seq.*
(By Plaintiff on behalf of the Nationwide Class, or, alternatively, the New York Subclass)

88. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

89. Defendants engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, by:

a. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass Members' PII; and

b. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and New York Subclass Members' PII including by implementing and maintaining reasonable security measures.

90. These omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII. Plaintiff and New York Subclass Members would have discontinued Defendants' access to their PII had this information been disclosed.

91. Defendants acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff's and New York Subclass Members' rights.

92. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

93. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the Data Breach.

94. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiff and the New York Subclass that they could not reasonably avoid.

95. Plaintiff and the New York Subclass seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

FOURTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
28 U.S.C. §§ 2201, *et seq.*
(By Plaintiff on behalf of the Nationwide Class)

96. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

97. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

98. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and statutory duties to reasonably safeguard its customers' sensitive personal information and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches. Plaintiff alleges that Defendants' data security practices remain inadequate.

99. Plaintiff and Class Members continue to suffer injury as a result of the compromise of their sensitive personal information and remain at imminent risk that further compromises of their personal information will occur in the future.

100. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendants continue to owe a legal duty to secure customers' sensitive personal information, to timely notify customers of any data breach, and to establish and implement data security measures that are adequate to secure customers' sensitive personal information.

101. The Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect consumers' sensitive personal information.

102. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, for which they lack an adequate legal remedy. The threat of another data breach is real, immediate, and substantial. If another data breach at Mr. Cooper occurs, Plaintiff and Class Members will not have an adequate remedy at law because not all of the resulting injuries are readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

103. The hardship to Plaintiff and Class Members if an injunction does not issue greatly exceeds the hardship to Defendants if an injunction is issued. If another data breach occurs, Plaintiff and Class Members will likely be subjected to substantial risk of identity theft and other damages. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants has a pre-existing legal obligation to employ such measures.

104. Issuance of the requested injunction will serve the public interest by preventing another data breach at Mr. Cooper, thus eliminating the additional injuries that would result to Plaintiff and the millions of customers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all other similarly situated, prays for relief as follows:

a. For an order certifying the Class(es) defined above and naming Plaintiff as representatives of the Class(es) and Plaintiff's attorneys as Class Counsel to represent the Class(es);

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For actual, compensatory, punitive, and nominal damages, in amounts to be determined by the trier of fact;

d. Declaratory and injunctive relief as described herein;

e. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

f. Awarding pre-and-post-judgment interest on any amounts awarded; and

g. Awarding such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial as to all issues triable by a jury.

Dated: November 20, 2023

/s/Roger L. Mandel

Roger L. Mandel
SBN 12891750
JEEVES MANDEL LAW GROUP, P.C.
2833 Crockett Street, Suite 135
Fort Worth, Texas 76107
rmandel@jeevesmandellawgroup.com
(214) 253-8300 - Telephone
(727) 822-1499 - Telecopier

Raymond P. Girnys *Will Apply for Admission Pro Hac Vice
Christian Levis *Will Apply for Admission Pro Hac Vice
Amanda G. Fiorilla *Will Apply for Admission Pro Hac Vice
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500

Email: rgirnys@lowey.com
Email: clevis@lowey.com
Email: afiorilla@lowey.com

Anthony M. Christina *Will Apply for Admission Pro Hac Vice
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA
Telephone: (215) 399-4770
Email: achristina@lowey.com

Attorneys for Plaintiff and the Proposed Class